REMARKS

Claim 1 is amended for purposes of expediting prosecution. Support for the amendment is provided by the example embodiments described in paragraphs [0017]-[0018], for example. Independent claims 9, 12, and 20 are amended to include limitations similar to those of claim 1. No new matter is believed to have been added. Claims 2, 3, 18, and 19 are cancelled without prejudice. Claims 1, 5-16, 20, and 22 are pending in the application.

In the discussion set forth below, Applicant does not acquiesce to any rejection or averment in the Office Action unless expressly stated. Applicant requests favorable reconsideration of the claims and withdrawal of the pending rejections in consideration of the present claim amendments and the following remarks.

Nonobviousness under 35 U.S.C. § 103

Claims 1-3, 5-16, 18-20, and 22 are believed to be patentable under 35 U.S.C. §103(a) over "Pang" (U.S. Patent No. 6,981,153 to Pang et al.) in view of "Lesea" (U.S. Patent No. 6,496,971 to Lesea et al.), further in view of "Weinlander" (U.S. Patent No. 5,991,858 to Weinlander). The rejection is respectfully traversed, because the Examiner has not established a *prima facie* case of obviousness. "The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." (MPEP §2142). Applicant respectfully submits that the evidence presented by the Examiner does not suggest all the claim limitations, nor has the Examiner presented a proper motivation for modifying Pang with teachings of Lesea and Weinlander.

According to claim 1, the system of securely using decryption keys during configuration of an integrated circuit having programmable logic, comprises a microcontroller within the integrated circuit for receiving an encrypted bitstream; a key storage register coupled to the microcontroller for storing key data; a decryptor coupled to the key storage register, wherein only the decryptor reads from the key storage register; and a configuration data register in the integrated circuit, wherein the configuration data register is readable by the microcontroller before the decryptor is

used and the configuration data register cannot be read by the microcontroller after the decryptor is used. Applicant respectfully submits that the Examiner has not shown that the Pang-Lesea-Weinlander combination suggests the claimed configuration data register that is readable by the microcontroller before the decryptor is used and that cannot be read by the microcontroller after the decryptor is used.

In the Office Action dated 7/9/2009 (OA 7-9-09) on page 3, the Examiner cited Pang's Fig. 3; col. 11, lines 44-56; and col. 14, lines 18-38 as teaching that the configuration data register cannot be read by the microcontroller after the decryptor is used. Applicant respectfully submits that the cited teachings do not suggest these limitations, nor are the added limitations suggested. Pang's Fig. 3 generally shows a configuration logic element 29. There is no apparent suggestion of any configuration data register that cannot be read by a microcontroller after the decryptor is used. Nor is there any apparent suggestion of the added limitations of allowing the microcontroller to read by the microcontroller the configuration data register before the decryptor is used.

Pang's col. 11, ll. 44-56 teaches the following:

> Configuration logic 29 includes the structures to support optional encryption as well as the structures to prevent design relocation and a single key attack. As shown in FIG. 6, configuration logic 29 includes a holding register 292, control logic 291, configuration registers (FDRI, FAR, CRC, and init CBC are shown), decryptor 24 interface multiplexers 294 and 295, 64-bit assembly register 297, and registers 298 and 299 (for interfacing with configuration access port 21). A 64-bit shift register 299 receives data from configuration access port 21, which can be a single pin for 1-bit wide data or 8 pins for 8-bit wide data. This data is loaded into 64-bit shift register 299 until register 299 is full.

Pang's col. 14, ll. 18-38 teaches the following:

> At step 88, this decrypted configuration data is sent on bus 27 (FIG. 3) to configuration logic 29. Configuration logic 29 calculates an updated cyclic redundancy check value to be compared with the cyclic redundancy value stored in the CRC register at the end of the loading process. If configuration logic 29 has been set to use encryption, a multiplexer in configuration logic 29 forwards this decrypted configuration data to the addressed column of configuration memory 12.
>
> At step 89 the counter is checked and if not finished, at step 96 the counter is decremented and the process returns to step 82 where the next 64 bits (2 words) are loaded from the bitstream.
>
> Finally, when step 89 indicates the counter is finished, at step 90, a CRC (cyclic redundancy check) value in the bitstream is compared with a CRC value calculated as

> the bitstream is loaded. If the values agree, configuration is complete and the FPGA goes into operation. If the values do not agree, a loading error has occurred and the entire configuration process is aborted.

Nothing in these cited teachings of Pang in any apparent manner suggests that a microcontroller is allowed to read a configuration data register before the decryptor is used to decrypt a bitstream and then not allowing the microcontroller to read from the configuration data register after the decryptor has decrypted the bitstream. If the rejection is maintained, Applicant respectfully requests that the Examiner explain how these teachings of Pang are construed to suggests these limitations. Otherwise, the rejection should be withdrawn.

As to claim 6, the claim recites that "the microcontroller further receives a configuration boot program comprising the decryptor in programmatic form along with the encrypted bitstream comprising encrypted configuration data to be loaded into the configuration data register." The Examiner has not shown that the Pang-Lesea-Weinlander combination suggests these limitations.

The Examiner cited Lesea's teachings at col. 8, lines 33-55 and Pang's teachings at col. 1, lines 31-38 and lines 52-58. However, none of these cited teachings makes any apparent mention of the decryptor program being received in the configuration boot program of a microcontroller. Lesea's col. 8, lines 33-55 teaches as follows:

> FIG. 5 is a flowchart of a method in accordance with another embodiment. After power-up, processor 9 reads a configuration mode code (step 300) from terminals M0, M1 and M2. If the configuration mode code has a particular value, then processor 9 executes a loader program (step 301) in RAM 12. Execution of this loader program causes processor 9 to configure IOBs such that a configuration program is read onto FPGA 1 and is loaded into RAM 12. The configuration program may be loaded into the FPGA in any number of ways. One way is to read the configuration program from an external PROM, one byte at a time as is done in the "master parallel mode" described above.
>
> After the loader program has loaded the configuration program into RAM 12, processor 9 executes the newly-loaded configuration program (step 302). Execution of this configuration program causes processor 9 to read configuration data onto the FPGA and to load that configuration data into the configuration memory cells of the FPGA, thereby configuring the FPGA for use as the desired user-specific circuit. A user is therefore able to provide a customized configuration mode by loading a customized configuration program into the FPGA and then causing processor 9 to execute that customized configuration program.

Lesea teaches that a loader program is loaded into an FPGA and execution of that loader program causes the processor to read configuration data into the FPGA and load the configuration data into the configuration memory cells. There is no apparent mention of the loader program including a decryptor program.

Pang's col. 1, lines 31-38 and lines 52-58 teach as follows:

> Many PLDs, particularly FPGAs, use volatile configuration memory that must be loaded from an external device such as a PROM every time the PLD is powered up. Since configuration data is stored external to the PLD and must be transmitted through a configuration access port, the privacy of the design can easily be violated by an attacker who monitors the data on the configuration access port, e.g. by putting probes on board traces.
>
> ...
>
> A key used for encrypting the design must somehow be communicated in a secure way between the PLD and the structure that decrypts the design, so the design can be decrypted by the PLD before being used to configure the PLD. Then, once the PLD has been configured using the unencrypted design, the design must continue to be protected from unauthorized discovery.

Pang teaches that configuration data may be loaded from a source external to the PLD and is prone to discovery by an attacker. Pang further teaches that the configuration data loaded into the PLD may be encrypted and decrypted on the PLD using a key which has been securely communicated to the PLD. As with Lesea, there is no apparent mention by Pang of the microprocessor receiving a configuration boot program that includes a decryptor program. If the rejection is maintained, Applicant respectfully requests that the Examiner explain how these teachings of Lesea and Pang are construed to suggest these limitations. Otherwise, the rejection should be withdrawn.

As to claim 8, the claim recites that "the microcontroller is an emulated microcontroller in the integrated circuit." The Examiner cited Pang's teachings at col. 5, lines 47-64 as suggesting these limitations. However, these cited teachings make no apparent mention of an emulated microcontroller. Pang's col. 5, lines 47-64 teaches as follows:

> Finally FPGA 10 includes configuration logic 14 for responding to a configuration bitstream from external source 15 on configuration access port 21 and for interfacing with JTAG logic block 13. The bitstream on configuration access port 21 is treated as words, in one embodiment 32-bit words. Several of the words, usually at or near the beginning of the bitstream, are used for setting up the configuration process and include, for example, length of a configuration memory frame, and starting address for the configuration data. Bus 19 allows communication between configuration logic 14 and JTAG logic block 13 so that the JTAG port can be used as another configuration access port. Bus 18 allows communication between configuration logic block 14 and configuration memory 12. In particular, it carries addresses to select configuration frames in memory 12, control signals to perform write and read operations, and data for loading into configuration memory 12 or reading back from configuration memory 12.

From the cited teachings, those skilled in the art will recognize that Pang teaches configuration logic that responds to a configuration bitstream and that interfaces with a JTAG block. There is no apparent mention of either a microcontroller or the microcontroller being emulated. Thus, the Examiner has not shown that the Pang-Lesea-Weinlander combination suggests these limitations. If the rejection is maintained, Applicant respectfully requests that the Examiner explain how these teachings of Lesea and Pang are construed to suggest these limitations. Otherwise, the rejection should be withdrawn.

Independent claims 9, 12, and 20 include limitations similar to those of claim 1. Claims 5 and 7 depend from claim 1, claims 10 and 11 depend from claim 9, claims 13-16 depend from claim 12, and claim 22 depends from claim 20. Therefore, the Examiner has not shown that the Pang-Lesea-Weinlander combination suggests these limitations for at least the reasons set forth above. Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1, 5-16, 20, and 22 is respectfully requested.

CONCLUSION

Reconsideration and a notice of allowance are respectfully requested in view of the amended claims and Remarks presented above. If the Examiner has any questions or concerns, a telephone call to the undersigned is invited.

Respectfully submitted,

/Lois D. Cartier/

Lois D. Cartier
Agent for Applicant
Reg. No. 40,941
(720) 652-3733

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent & Trademark Office on July 27, 2009.
/susan wiens/
Typed Name: Susan Wiens